High Confidence Software and Systems (HCSS)

NITRD Agencies: NSF, OSD and DoD Service research organizations, NIH, DARPA, NSA, NASA, NIST
Other Participants: DHS, DOE (OE), FAA, FDA

The goal of HCSS R&D is to bolster the Nation's capability and capacity for engineering effective and efficient distributed, real-time, IT-centric systems that are certifiably and inherently dependable, reliable, safe, secure, fault-tolerant, survivable, and trustworthy. These systems, which are often embedded in larger physical and IT systems, are essential for the operation and evolution of the country's national defense, key industrial sectors, and critical infrastructures.

President's 2007 Request

Strategic Priorities Underlying This Request
Demand for new classes of computationally enabled, adaptive, distributed, embedded, and real-time systems for mission- and safety-critical applications. Research is needed to develop:

Next-generation capabilities: Complex new capabilities and foundations for advances in physical and engineered systems for Federal missions and U.S. industrial innovation in key areas such as:
- **Aerospace systems:** Aircraft autonomy, future airspace operations, human-rated space systems
- **Automotive systems:** "Drive-by-wire" and intelligent vehicle and highway systems
- **Critical infrastructure systems:** Beyond supervisory control and data acquisition (SCADA), power grid automation, water management, supply chain integration
- **Defense systems:** Real-time, distributed, embedded systems in a highly network-centric environment for applications ranging from counterterrorism to ballistic and cruise missile defense
- **Medical care:** "Operating room of the future," telemedicine, medical devices, paramedic support systems

New high-confidence enabling technologies: Revolutionary paradigms to replace today's operating systems (OSs), middleware (MW), and virtual machines (VMs) that integrate complex mechanisms and enable fault tolerance, dynamic adaptation, partitioning for fault isolation, real-time scheduling, and security

Assurance for complex, integrated systems: New systems built on a principled framework and a new computing technology base for integrating assured concepts that can replace today's inadequate technologies, which were designed for benign environments and noncritical applications and are underpinned by a fragmented collection of theories. Priority research topics include:
- **Scientific foundations:** Software and systems assurance
- **Design and engineering advances:** Model-based system design, formal methods, correct-by-construction techniques, and tools for designing, testing, verifying, and validating systems with software as key components, in part to expand the types of software-intensive systems that can be confidently deployed
- **Assurance measures and metrics:** Ability to justify the degree of confidence in established properties

Highlights of Request

High-confidence, real-time operating systems (RTOS), MW, and VMs: Continue examination of adequacy of current real-time OS, MW, and VM technologies to identify R&D needed to achieve a next-generation high-confidence RTOS technology base; foster university/industry/government R&D partnership; launch a multiagency effort in high-confidence RTOS software, systems, and assurance – NSF, NSA, NIST, OSD (ODDR&E), DoD (AFRL), with NASA, DOE (OE), FAA, FDA, DoD (ONR, USASMDC/ARSTRAT)

Science of Design (SoD): Basic research in design of software-intensive systems that imports and adapts creative scientific ideas from other design fields (e.g., engineering, urban planning, economics, the arts) – NSF

Assured information systems: R&D toward an intelligent, secure flexible, self-protecting global infrastructure; robust protection mechanisms to support sharing of information across diverse communities; development of safe computing platforms that can securely isolate, measure, and attest to correct operations; cryptographic algorithms and engineering to protect the content of information systems – NSA

Verification Grand Challenge: Develop deployable high-assurance technologies for large-scale software systems; begin by convening panels of specialists (i.e., integrated verification systems, theory, system certification) to identify research directions, propose action plan, and suggest projects – NSA, NSF

Deployed and near-term SCADA and industrial control systems: Develop requirements, standards, software assurance metrics, and guidelines – NIST, DHS

Software assurance metrics, tools, evaluation, **and databases** – NIST, NSA, DHS

Planning and Coordination Supporting Request

High-confidence RTOS technology needs assessments and national roadmapping workshop: Non-disclosure briefings by technology development and systems integration vendors, academic researchers, and RTOS standards organization; initiate university/industry/government partnership; convene workshop(s) to roadmap RTOS R&D – NSF, DoD (AFRL), NIST, NSA, with DoD (ONR, USASMDC/ARSTRAT), OSD (ODDR&E), NASA, DOE (OE), FAA, FDA

High Confidence Medical Device Software and Systems: Ongoing national workshop series – NSF, NSA, with NIST, FDA

Software for Critical Aviation Systems: Begin workshop series – NSF, DoD (AFRL), NSA, with NASA, FAA

Beyond SCADA and Distributed Control Systems: Begin national workshop series on high-confidence devices and software to enable, protect, and evolve critical infrastructures – NSF, NIST, NSA, OSD (ODDR&E), with DoD (AFRL), DHS, DOE (OE)

Black boxes for medical devices: Preliminary study of the benefits of building data recording technologies into medical device systems to provide complete detailed records about their operation for analysis of processes and state prior to and during failures – NSF, with FDA

Open-source software for high-confidence medical devices: Exploration of future directions and practices for certification – NIH, NSF, FDA, other agencies

Sixth annual HCSS conference – NSA, with other HCSS agencies

National Voluntary Lab Accreditation Program (NVLAP): Calibration and/or test methods, protocols, and standards to meet accreditation needs for a variety of products and processes – NIST, NSA

Software Assurance Metrics and Tool Evaluation Workshops: Bring together users, developers of software assurance tools, compare effectiveness of tools and techniques, develop taxonomies of vulnerabilities and tools, and expand a software security assurance standard reference database – NIST, DHS, with other agencies

Sufficient Evidence? Building Certifiably Dependable Systems: Complete National Academies/CSTB study assessing current practices for developing and evaluating mission-critical software – NSF, NSA, DoD (ONR), FAA, with DARPA, DoD (ARO), NASA, NIST, FDA

Additional 2006 and 2007 Activities by Agency

NSF: Fundamental research in distributed, real-time, and embedded systems; operating systems; hybrid discrete and continuous control systems; formal methods for composition and verification; rigorous models of computation; compositional software methods; critical infrastructure component of Cyber Trust

DoD (AFRL): Technology for affordable, safe software; certification technologies for advanced flight-critical systems project; high-confidence design of distributed, embedded systems; advocate high-assurance security architecture for embedded systems

OSD (ODDR&E): Software Engineering Institute research – designs for networked systems that recognize, resist, and recover quickly from attacks; quality attribute reasoning; software architectures and practices that enable automated support, predict runtime behavior of software, and select software components based on certified properties and predicted contribution to assembly behavior; principles, methods, techniques for integration and interoperation across components, systems, systems of systems; model-based software engineering for real-time systems; methods for evidence-based assurance

NASA: Exploration systems – tools and techniques that support cost effective development and verification for autonomous and adaptive systems; aeronautics research – enabling technologies for integrated vehicle health management, integrated intelligent flight deck, and integrated resilient aircraft control sub-elements

NIST: Software diagnostic and conformance tests, tools, and methods; source code analysis tools; National Software Reference Library; voting accuracy standards; software engineering method development

FAA: Certifiably dependable systems, including software certification and incremental certification in traditional safety-critical systems; enhanced methods and standards for engineering security into products and improved continuous external monitoring of a system's internal vital signs; improved continuous security risk assessment in complex networked environment

FDA: Formal-methods-based design, including safety models, forensics, and design for infusion pumps, and blood bank regulatory policy models and certification; architecture, platform, middleware, and resource management, including plug-and-play in the operating room of the future